

10/549293

DOCKET NO.: 277771US6PCT

JC17 Rec'd PCT/PTO 16 SEP 2005

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Munetake EBIHARA, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/06900

INTERNATIONAL FILING DATE: May 14, 2004

FOR: INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING  
DEVICE AND METHOD

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119  
AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that  
the applicant claims as priority:

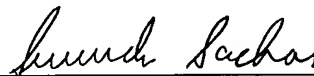
**COUNTRY**  
Japan

**APPLICATION NO**  
2003-150906

**DAY/MONTH/YEAR**  
28 May 2003

Certified copies of the corresponding Convention application(s) were submitted to the  
International Bureau in PCT Application No. PCT/JP04/06900. Receipt of the certified  
copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been  
acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Gregory J. Maier  
Attorney of Record  
Registration No. 25,599  
Surinder Sachar  
Registration No. 34,423

Customer Number  
**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

14. 5. 2004

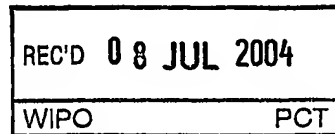
日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2003年 5月28日

出願番号  
Application Number: 特願2003-150906  
[ST. 10/C]: [JP2003-150906]



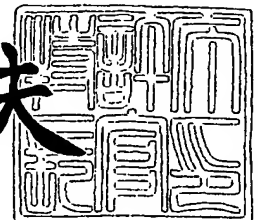
出願人  
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 6月17日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0390369803

【提出日】 平成15年 5月28日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 9/06  
G06F 3/06  
G09C 1/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 海老原 宗毅

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 勝股 充

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 久野 浩

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 林 隆道

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録媒体、並びに情報処理装置及び方法

【特許請求の範囲】

【請求項 1】 第 1 の実行ファイルが複製不可に記録された情報記録媒体であって、

上記第 1 の実行ファイルは、第 2 の実行ファイルとの間で認証処理を行う認証手段と、該第 1 の実行ファイルに固有の固有鍵情報を取得する鍵取得手段と、上記固有鍵情報を上記第 2 の実行ファイルに送信する送信手段とを有し、上記情報記録媒体が情報処理装置に挿入されたときに実行される

ことを特徴とする情報記録媒体。

【請求項 2】 上記固有鍵情報は、コンテンツを暗号化する暗号鍵情報を暗号化するために用いられることを特徴とする請求項 1 記載の情報記録媒体。

【請求項 3】 上記第 2 の実行ファイル又は上記コンテンツは、上記情報記録媒体、上記情報処理装置又は他の情報処理装置に記録されていることを特徴とする請求項 2 記載の情報記録媒体。

【請求項 4】 上記コンテンツは、上記情報記録媒体に記録されており、

上記固有鍵情報は、上記コンテンツに付属する署名情報を暗号化する暗号鍵情報を暗号化するために用いられ、

上記送信手段は、上記署名情報に基づいて上記コンテンツを上記第 2 の実行ファイルに送信する

ことを特徴とする請求項 3 記載の情報記録媒体。

【請求項 5】 第 1 の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置であって、

暗号化されたコンテンツを再生する第 2 の実行ファイルを有し、

上記第 2 の実行ファイルは、上記第 1 の実行ファイルとの間で認証処理を行う認証手段と、上記第 1 の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成手段と、上記暗号鍵情報を用いて上記暗号化されたコンテンツを復号化する復号化手段と、復号化した上記コンテンツを再生する再生手段とを有し、上記情報記録媒体が挿入されたときに実行される

ことを特徴とする情報処理装置。

【請求項 6】 上記暗号化されたコンテンツは、上記情報記録媒体、上記情報処理装置又は他の情報処理装置に記録されていることを特徴とする請求項 5 記載の情報処理装置。

【請求項 7】 上記暗号化されたコンテンツは、上記情報記録媒体に記録されており、

上記固有鍵情報は、上記暗号化されたコンテンツに付属する署名情報を暗号化する暗号鍵情報を暗号化するために用いられ、

上記第 2 の実行ファイルは、上記署名情報に基づいて上記第 1 の実行ファイルから上記暗号化されたコンテンツを受信する受信手段を有する

ことを特徴とする請求項 6 記載の情報処理装置。

【請求項 8】 第 1 の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置の情報処理方法であって、

上記第 1 の実行ファイルとの間で認証処理を行う認証工程と、

上記第 1 の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成工程と、

上記暗号鍵情報を用いて暗号化されたコンテンツを復号化する復号化工程と、

復号化した上記コンテンツを再生する再生工程と

を有することを特徴とする情報処理方法。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、コンテンツの不正利用を防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする情報記録媒体、並びにそのような情報記録媒体を用いてコンテンツを再生する情報処理装置及びその方法に関する。

##### 【0002】

##### 【従来の技術】

近年において、光ディスク等の情報記録媒体の大容量化と普及により、記録さ

れている情報の著作権を保護するために、不法なコピーの防止が重要とされてきている。すなわち、オーディオデータやビデオデータの場合には、コピー或いはダビングにより劣化のない複製物を容易に生成でき、またコンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのが実情である。

#### 【0003】

このようなことから、上記不法コピーの防止を目的として、コピーコントロールCD (Copy Control Compact Disk; C C C D) と称されるレッドブック規格外の音楽CDが開発・販売されるに至っている。このC C C Dのセカンドセッションエリアに記録されているオーディオデータについては、C C C D上に記録されている専用の再生モジュールを用いてパーソナルコンピュータでの再生が可能であるものの、パーソナルコンピュータ内部へ取り込み（リッピング）ができず、コピーが防止されるようになされている。

#### 【0004】

また、同様に不法コピーの防止を目的として、S e c u R O M（登録商標）と称されるCD-ROM (Compact Disk - Read Only Memory) も開発・販売されている。このS e c u R O Mでは、サブコード（Qサブチャンネル）に隠蔽されたコピー防止キーを抽出し、該コピー防止キーを用いて、少なくともその一部が暗号化されたアプリケーションを復号化することで、該アプリケーションを実行することができるものの、不法コピーされている場合には、アプリケーションを暗号化したコピー防止キーとは異なるものが抽出され、該アプリケーションを実行することができない。

#### 【0005】

##### 【特許文献1】

特開平11-250512号公報

#### 【0006】

##### 【発明が解決しようとする課題】

しかしながら、このような従来のC C C DやS e c u R O M（登録商標）においては、媒体とそれに記録された音楽情報（コンテンツ）とが不可分であるため

、コンテンツを媒体から切り離して運用することができず、運用の柔軟性がないという問題があった。また、媒体のコピー防止技術を改良しようとした場合、その媒体に記録されたコンテンツを再生するパーソナルコンピュータ等にインストールしなければならないソフトウェアが複雑化してしまう虞があった。

#### 【0007】

本発明は、このような従来の実情に鑑みて提案されたものであり、コンテンツの不正利用を防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする情報記録媒体、並びにそのような情報記録媒体を用いてコンテンツを再生する情報処理装置及びその方法を提供することを目的とする。

#### 【0008】

##### 【課題を解決するための手段】

上述した目的を達成するために、本発明に係る情報記録媒体は、第1の実行ファイルが複製不可に記録された情報記録媒体であり、この第1の実行ファイルは、第2の実行ファイルとの間で認証処理を行う認証手段と、該第1の実行ファイルに固有の固有鍵情報を取得する鍵取得手段と、上記固有鍵情報を上記第2の実行ファイルに送信する送信手段とを有し、情報記録媒体が情報処理装置に挿入されたときに実行されるものである。

#### 【0009】

このような情報記録媒体に記録された第1の実行ファイルは、情報記録媒体が情報処理装置に挿入されたときに実行され、第2の実行ファイルとの間で相互に認証処理を行い、第1のファイルに固有の固有鍵情報を第2のファイルに送信する。

#### 【0010】

また、上述した目的を達成するために、本発明に係る情報処理装置は、第1の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置であって暗号化されたコンテンツを再生する第2の実行ファイルを有し、この第2の実行ファイルは、上記第1の実行ファイルとの間で認証処理を行う認証手段と、上記第1の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成



する鍵生成手段と、上記暗号鍵情報を用いて上記暗号化されたコンテンツを復号化する復号化手段と、復号化した上記コンテンツを再生する再生手段とを有し、上記情報記録媒体が挿入されたときに実行されるものである。

#### 【0011】

このような情報処理装置が有する第2の実行ファイルは、第1の実行ファイルが複製不可に記録された情報記録媒体が挿入されたときに実行され、第1の実行ファイルとの間で相互に認証処理を行い、第1のファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生する。

#### 【0012】

また、上述した目的を達成するために、本発明に係る情報処理方法は、第1の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置の情報処理方法であり、上記第1の実行ファイルとの間で認証処理を行う認証工程と、上記第1の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成工程と、上記暗号鍵情報を用いて暗号化されたコンテンツを復号化する復号化工程と、復号化した上記コンテンツを再生する再生工程とを有するものである。

#### 【0013】

このような情報処理方法では、情報記録媒体に記録された第1の実行ファイルとの間で相互に認証処理を行い、第1のファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生する。

#### 【0014】

##### 【発明の実施の形態】

以下、本発明を適用した具体的な実施の形態について、図面を参照しながら詳細に説明する。

#### 【0015】

まず、本実施の形態の概念構成について、図1を用いて説明する。図1において、鍵取得モジュール2（第1の実行ファイル）は、コピー防止技術が施された

読み取り専用の情報記録媒体 1 に記録されている。このコピー防止技術としては、例えば S e c u R O M（登録商標）に用いられている技術や、いわゆるダミーファイル法の技術が挙げられるが、これらに限定されず種々の技術を用いることができる。再生モジュール 3（第 2 の実行ファイル）は、この鍵取得モジュール 2 から該鍵取得モジュール 2 に固有のメディア鍵（固有鍵情報）を安全に取得し、このメディア鍵からコンテンツ鍵（暗号鍵情報）を生成し、このコンテンツ鍵を用いて暗号化コンテンツ 4 を復号化して再生する。

#### 【0016】

このように、本実施の形態では、コンテンツが暗号化された状態で提供され、その暗号化コンテンツ 4 の復号化に用いられるメディア鍵がコピー防止技術の施された情報記録媒体 1 に記録されているため、暗号化コンテンツ 4 がコピーされた場合であっても正規の情報記録媒体 1 がなければメディア鍵を取得できず、コンテンツを利用することができない。

#### 【0017】

ここで、本実施の形態における鍵取得モジュール 2 は情報記録媒体 1 上に存在する必要があるが、再生モジュール 3 及び暗号化コンテンツ 4 は情報記録媒体 1 上に存在する必要はなく、情報記録媒体 1 の外部に存在していても構わない。つまり、再生モジュール 3 及び暗号化コンテンツ 4 の配置形態としては、

- 1) 情報記録媒体 1 上に再生モジュール 3 及び暗号化コンテンツ 4 が存在する場合、
- 2) 情報記録媒体 1 の外部に再生モジュール 3 及び暗号化コンテンツ 4 が存在する場合、
- 3) 情報記録媒体 1 上に再生モジュール 3 が存在し、情報記録媒体 1 の外部に暗号化コンテンツ 4 が存在する場合、
- 4) 情報記録媒体 1 の外部に再生モジュール 3 が存在し、情報記録媒体 1 上に暗号化コンテンツ 4 が存在する場合、

の 4 通りが考えられる。

#### 【0018】

以下では、再生モジュール 3 及び暗号化コンテンツ 4 が情報記録媒体 1 の挿入

される情報処理装置に存在する場合（上記2の場合）について、主として説明する。この再生モジュール3及び暗号化コンテンツ4は、予めネットワークを介して情報処理装置にダウンロードしたものであっても構わない。なお、以下では、情報記録媒体1は読み出し専用の光ディスクであるものとする。

#### 【0019】

先ず、情報記録媒体1のコピー防止技術としてSecuROM（登録商標）の技術が用いられている場合に、鍵取得モジュール2がメディア鍵を取得し、このメディア鍵を再生モジュール3に転送するまでの処理を図2のフローチャートに示す。

#### 【0020】

このSecuROM（登録商標）の技術とは、簡単には、予め情報記録媒体1上の所定のアドレス及び個数のサブコード（Qサブチャンネル）を変更しておき、アプリケーションを暗号化するコピー防止キーとしてその変更パターンを用いるものである。アプリケーションを実行する際には、上記所定のアドレス及び個数のQサブチャンネルを検索し、その変更パターンからコピー防止キーを抽出する。ここで、情報記録媒体1をコピーした場合、変更が施されていた正規でないQサブチャンネルは正規のQサブチャンネルとしてコピーされる。この結果、元々アプリケーションを暗号化していたものとは異なるコピー防止キーが抽出されることとなり、アプリケーションを復号化して実行することができない。なお、この図2に示すコピー防止技術については、例えば特開平11-250512号公報に記載されている。

#### 【0021】

具体的には、始めに図2のステップS1において、鍵取得モジュール2は、暗号化されていない例えば前半部分のプログラムにより、情報記録媒体1上の所定のアドレス及び個数のサブコード（Qサブチャンネル）をスキャンし、ステップS2において、そのQサブチャンネルが正規であるか否かを検索する。次にステップS3において、鍵取得モジュール2は、正規でないQサブチャンネルの数に応じてコピー防止キーを抽出する。そしてステップS4では、抽出したコピー防止キーを用いて鍵取得モジュール2の後半部分の暗号を復号化できるか否かが判

別される。ステップ S 4 において復号化できる場合 (Yes) にはステップ S 5 に進み、復号化できない場合 (No) には処理を終了する。ステップ S 5 において、鍵取得モジュール 2 は、再生モジュール 3 との間で認証処理を行い、ステップ S 6 では、認証の適否が判別される。ステップ S 6 において相互に認証しない場合 (No) には処理を終了し、相互に認証する場合 (Yes) にはステップ S 7 においてメディア鍵を再生モジュール 3 に転送する。

#### 【0022】

一方、情報記録媒体 1 のコピー防止技術としていわゆるダミーファイル法の技術が用いられている場合に、鍵取得モジュール 2 がメディア鍵を取得し、このメディア鍵を再生モジュール 3 に転送するまでの処理を図 3 のフローチャートに示す。

#### 【0023】

このダミーファイル法の技術とは、簡単には、情報記録媒体 1 のサイズよりも大きいダミーファイルが実際に情報記録媒体 1 に記録されているかのように予めディレクトリレコードを変更しておき、アプリケーションを実行する際にそのダミーファイルのサイズを検査するものである。この情報記録媒体 1 をコピーする場合には、例えばディレクトリレコードのダミーファイルサイズを実際のダミーファイルのサイズに一致させる必要があるが、アプリケーションの実行前にそのダミーファイルのサイズが元のサイズ (情報記録媒体 1 のサイズよりも大きいサイズ) と一致するか否かが検査され、一致しない場合にはアプリケーションの実行が許可されない。なお、この図 3 に示すコピー防止技術については、例えば特開 2001-229019 号公報に記載されている。

#### 【0024】

具体的には、始めに図 3 のステップ S 10 において、鍵取得モジュール 2 はダミーファイルを開き、ステップ S 11 において、そのダミーファイルのファイルサイズを検査する。次にステップ S 12 において、鍵取得モジュール 2 は、そのファイルサイズが元のファイルサイズと一致するか否かを判別し、一致しない場合 (No) には処理を終了する。一方、一致する場合 (Yes) にはステップ S 13 に進む。ステップ S 13 において、鍵取得モジュール 2 は、再生モジュール 3 と

の間で認証処理を行い、ステップS 14では、認証の適否が判別される。ステップS 14において相互に認証しない場合 (No) には処理を終了し、相互に認証する場合 (Yes) にはステップS 15においてメディア鍵を再生モジュール3に転送する。

#### 【0025】

次に、再生モジュール3が鍵取得モジュール2から鍵を取得し、暗号化コンテンツ4を復号化して再生するまでの処理を図4のフローチャートに示す。ステップS 20において、再生モジュール3は、鍵取得モジュール2がロード可能であるか否かを判別し、ロード可能でない場合 (No) には処理を終了し、ロード可能である場合 (Yes) にはステップS 21に進む。次にステップS 21において、再生モジュール3は、鍵取得モジュール2との間で認証処理を行い、ステップS 22では、認証の適否が判別される。ステップS 22において相互に認証しない場合 (No) には処理を終了し、相互に認証する場合 (Yes) にはステップS 23において鍵取得モジュール2からメディア鍵を取得する。

#### 【0026】

続いてステップS 24において、再生モジュール3は、取得したメディア鍵からコンテンツ鍵を生成し、ステップS 25において、このコンテンツ鍵を用いて暗号化コンテンツ4の復号化を行う。なお、この暗号化コンテンツ4は、情報記録媒体1が挿入される情報処理装置内に存在するものであっても、ネットワークを介してダウンロードしたものであっても構わない。そしてステップS 26において、コンテンツを再生可能であるか否かが判別され、再生不可である場合 (No) には処理を終了し、再生可能である場合 (Yes) にはステップS 27でコンテンツを再生する。

#### 【0027】

なお、上述した図4では、暗号化コンテンツ4を再生する場合について説明したが、情報記録媒体1に暗号化コンテンツ4が記録されている場合には、この暗号化コンテンツ4を情報処理装置にインポートすることも可能である。このような場合において、再生モジュール3が鍵取得モジュール2から鍵を取得し、暗号化コンテンツ4を情報処理装置にインポートするまでの処理を図5のフローチャ

ートに示す。なお、ステップ S 3 4 においてコンテンツ鍵を生成するまでの処理は上述した図 4 と同様であるため説明を省略する。

#### 【0028】

ステップ S 3 5 において、再生モジュール 3 は、生成したコンテンツ鍵を用いて、例えば暗号化コンテンツ 4 に付属する権利情報及び暗号署名のうち、暗号署名を復号化して権利情報の検証を行う。なお、この権利情報及び暗号署名は、情報記録媒体 1 上に存在するものであっても、ネットワークを介してダウンロードしたものであっても構わない。そしてステップ S 3 6 において、インポートが許可されるか否かが判別され、インポートが許可されない場合 (No) には処理を終了し、インポートが許可される場合 (Yes) にはステップ S 3 7 で暗号化コンテンツ 4 をインポートする。

#### 【0029】

以下、上述した情報処理装置の具体的な構成例について図 6 を用いて説明する。図 6 に示すように、情報処理装置 10 は、該情報処理装置 10 の各部を統括して制御する CPU (Central Processing Unit) 11 と、不揮発性のメモリである ROM (Read Only Memory) 12 と、揮発性のメモリである RAM (Random Access Memory) 13 と、通信処理を行う通信部 14 と、図示しないハードディスクに対して各種データの書き込み及び／又は読み出しを行う HDD (Hard Disk Drive) 15 と、音声を出力する出力部 16 と、情報記録媒体 1 に対して各種データの書き込み及び／又は読み出しを行うインターフェース (I/F) 部 17 とがバス 18 を介して相互に接続されてなる。

#### 【0030】

CPU 11 は、例えば ROM 12 に記録されているプログラムに従って、プログラムを実行するための制御を行う。RAM 13 には、CPU 11 が各種処理を実行する上で必要なプログラムやデータが必要に応じて一時的に格納される。

#### 【0031】

通信部 14 は、例えばモデムやターミナルアダプタ等により構成され、電話回線を介してインターネットに接続される。

#### 【0032】

HDD 15 は、図示しないハードディスクからデータの読み出しを行うほか、例えば通信部 14 を介して入力したデータの書き込みを行う。

#### 【0033】

オーディオ出力部 16 は、例えば通信部 14 を介して入力したオーディオデータや、インターフェース部 17 を介して情報記録媒体 1 から入力したオーディオデータに対して、必要に応じて変換を施して出力する。

#### 【0034】

インターフェース部 17 は、CPU 11 の制御のもとに、情報記録媒体 1 に対してデータを入出力するタイミングを調整し、データの形式を変換する。

#### 【0035】

このような情報処理装置 10 において、再生モジュール 3 は、例えば HDD 15 に記録されており、情報記録媒体 1 に記録された鍵取得モジュール 2 との間で上述した処理を行い、メディア鍵を取得する。そして、再生モジュール 3 は、このメディア鍵からコンテンツ鍵を生成し、このコンテンツ鍵を用いて、例えば通信部 14 を介して入力して HDD 15 に記録された暗号化コンテンツ 4 を復号化する。復号化されたコンテンツは、CPU 11 の制御のもと、オーディオ出力部 16 から出力される。

#### 【0036】

以上説明したように、本実施の形態における情報記録媒体 1 及び情報処理装置 10 によれば、コンテンツが暗号化された状態で提供され、その暗号化コンテンツ 4 の復号化に用いられるメディア鍵がコピー防止技術の施された情報記録媒体 1 に記録されているため、暗号化コンテンツ 4 がコピーされた場合であっても正規の情報記録媒体 1 がなければメディア鍵を取得できず、コンテンツを利用することができない。これにより、コンテンツの保護が図られる。

#### 【0037】

特に、暗号化コンテンツ 4 は情報記録媒体 1 上に存在する必要はなく、情報記録媒体 1 の外部に存在していても構わないため、情報記録媒体 1 の購入者のみが復号化できるような暗号化コンテンツ 4 をネットワークを介して配布するなど、コンテンツの柔軟な運用が可能となる。

## 【0038】

また、再生モジュール2は、鍵取得モジュール1からメディア鍵を取得し、そのメディア鍵からコンテンツ鍵を生成して暗号化されたコンテンツを復号化するのみであり、情報記録媒体1にどのようなコピー防止技術が施されているかには依存しないため、コピー防止技術を改良した場合に、情報処理装置10に新たなソフトウェア等をインストールする必要がない。

## 【0039】

なお、本発明は上述した実施の形態のみに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。

## 【0040】

例えば、上述の実施の形態では、コンテンツがオーディオデータであるものとして説明したが、これに限定されるものではなく、ビデオデータなど他種のデータであっても構わない。

## 【0041】

## 【発明の効果】

以上詳細に説明したように、本発明に係る情報記録媒体、並びに情報処理装置及びその方法によれば、情報記録媒体に複製不可に記録された第1の実行ファイルと第2の実行ファイルとの間で相互に認証処理を行った後、第1の実行ファイルから第2の実行ファイルに固有鍵情報を送信し、第2の実行ファイルでは、この固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生することにより、コンテンツの不正利用が防止されると共に、コンテンツの柔軟な運用が可能となり、さらにコピー防止技術の改良も容易となる。

## 【図面の簡単な説明】

## 【図1】

本実施の形態の概念構成を説明する図である。

## 【図2】

鍵取得モジュールがメディア鍵を取得して再生モジュールに転送するまでの処理の一例を説明するフローチャートである。



**【図 3】**

鍵取得モジュールがメディア鍵を取得して再生モジュールに転送するまでの処理の他の例を説明するフローチャートである。

**【図 4】**

再生モジュールが鍵取得モジュールから鍵を取得し、暗号化コンテンツを復号化して再生するまでの処理を説明するフローチャートである。

**【図 5】**

再生モジュールが鍵取得モジュールから鍵を取得し、暗号化コンテンツを情報処理装置にインポートするまでの処理を説明するフローチャートである。

**【図 6】**

本実施の形態における情報処理装置の構成例を示す図である。

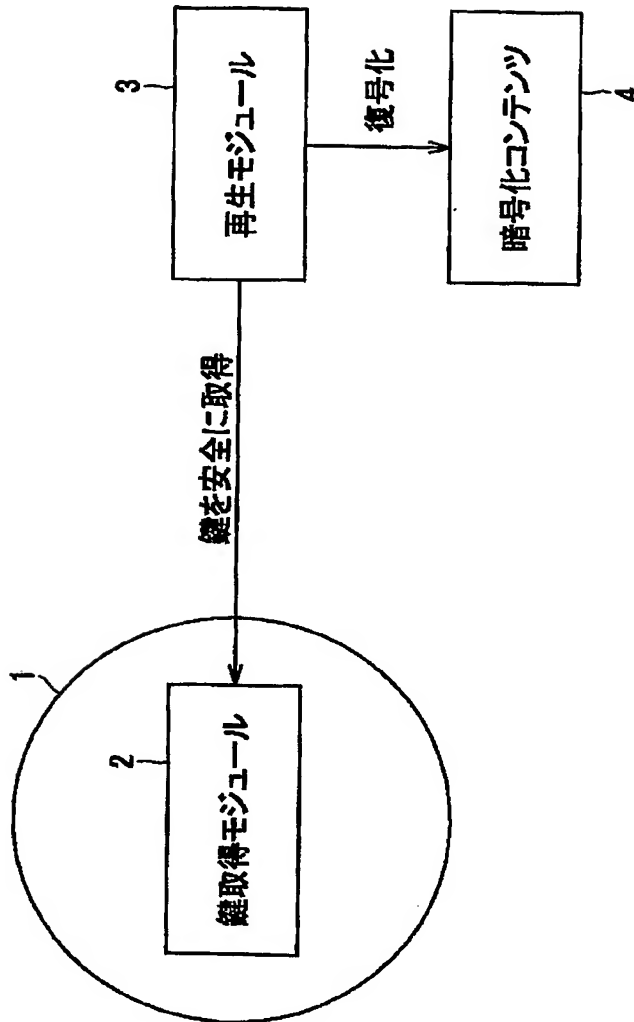
**【符号の説明】**

1 情報記録媒体、2 鍵取得モジュール、3 再生モジュール、4 暗号化コンテンツ、10 情報処理装置

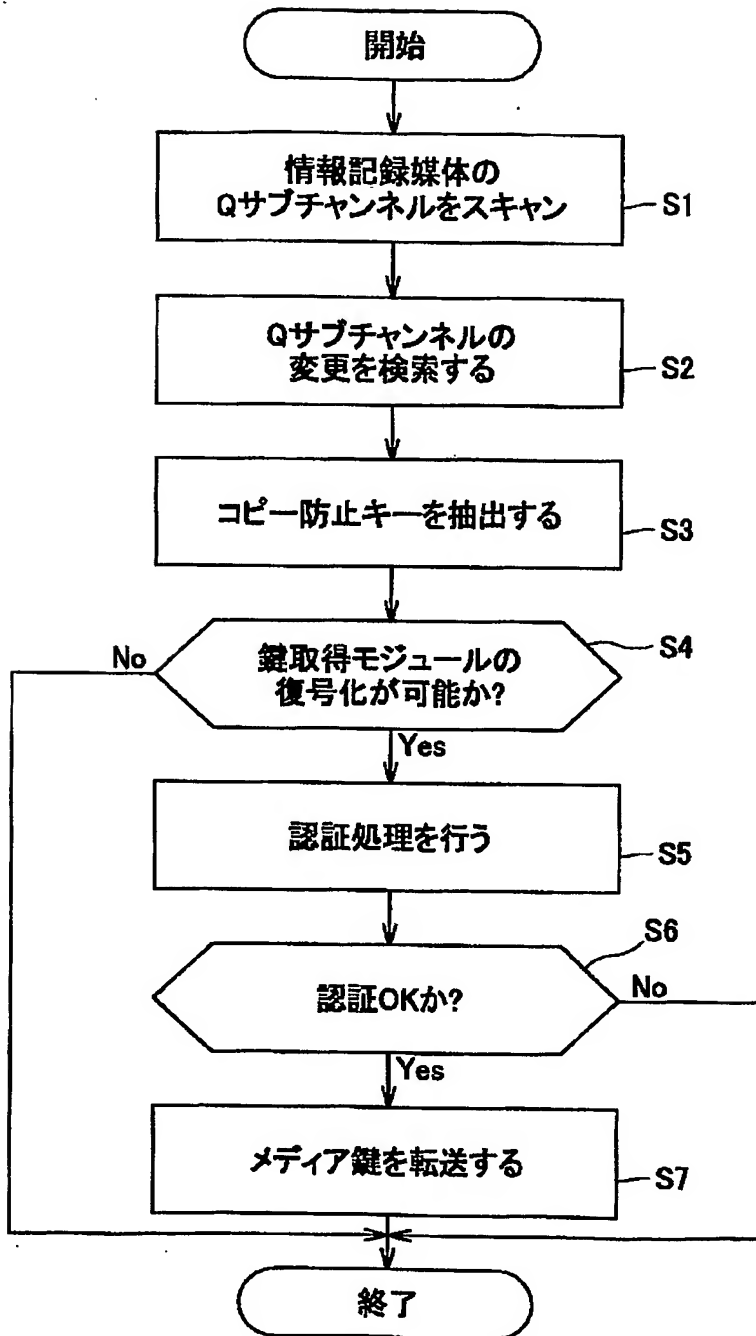
【書類名】

図面

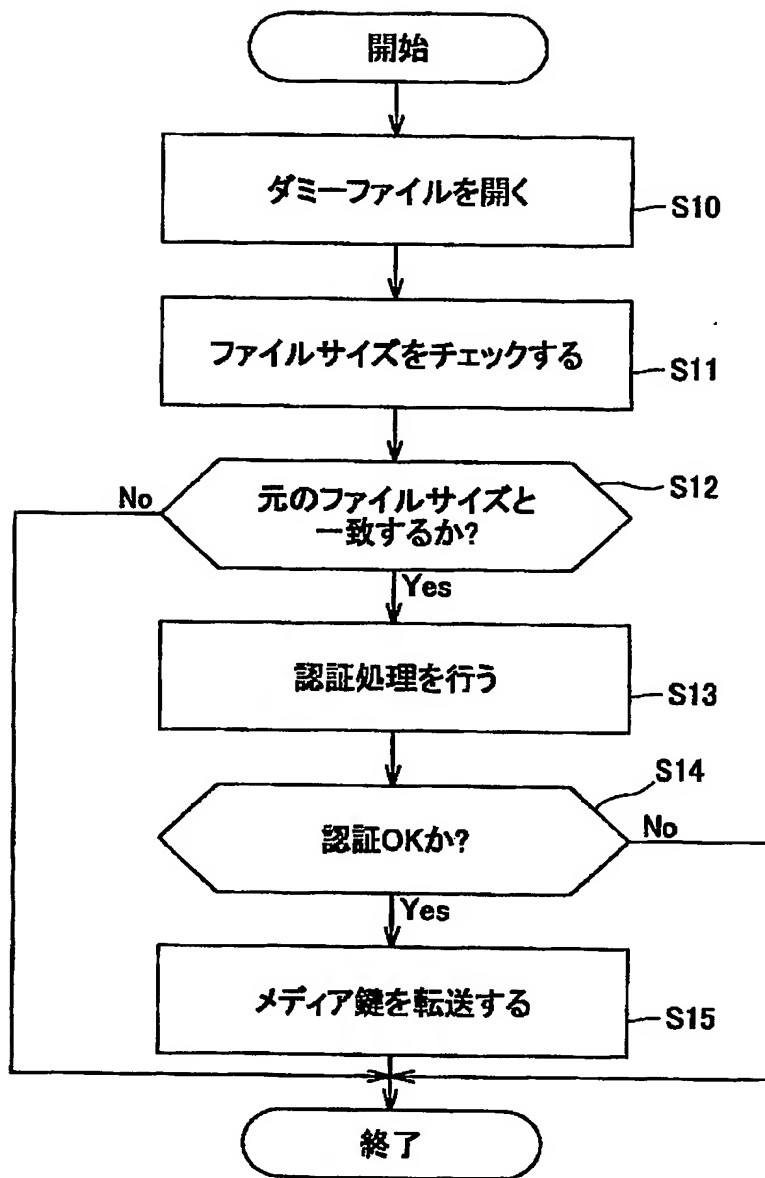
【図 1】



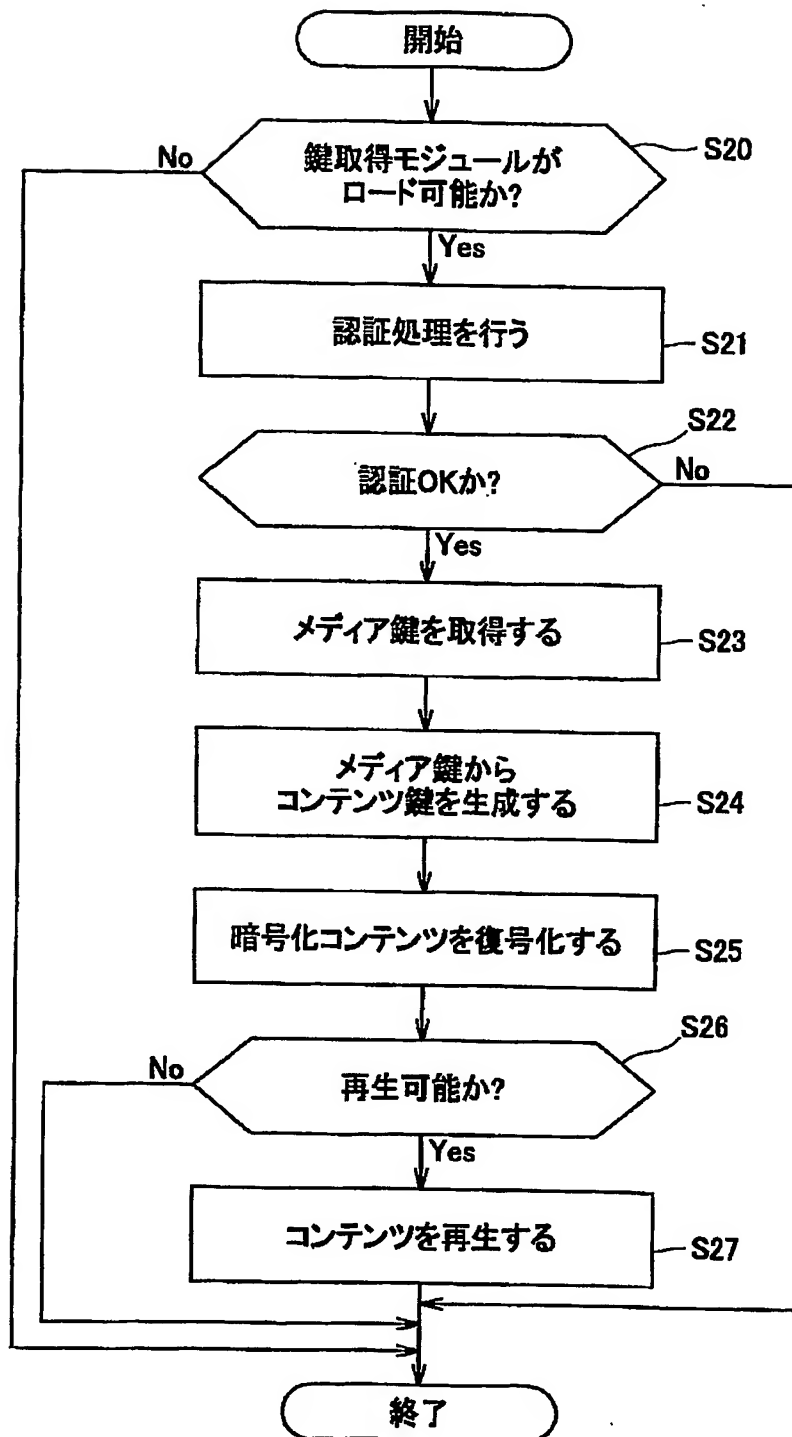
【図 2】



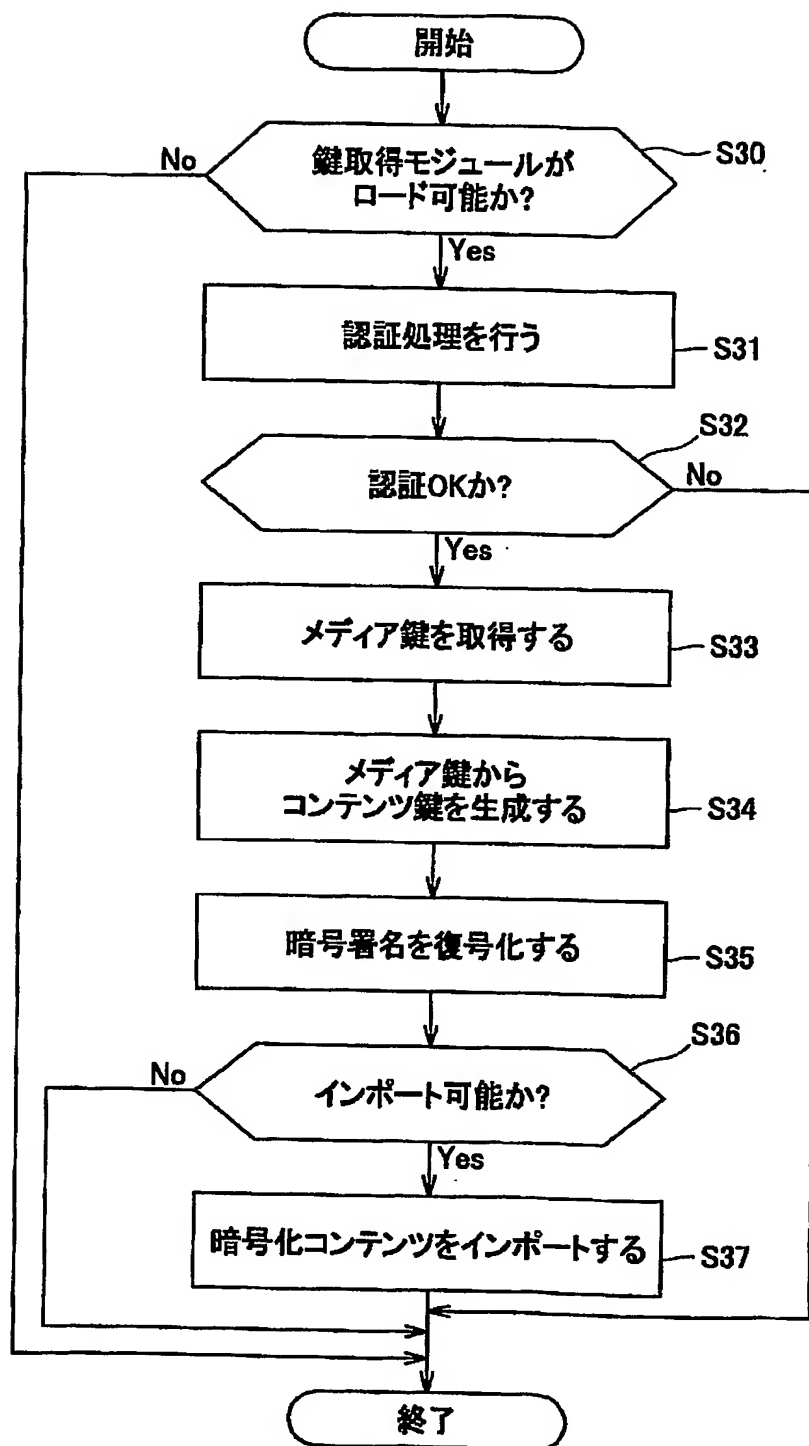
【図 3】



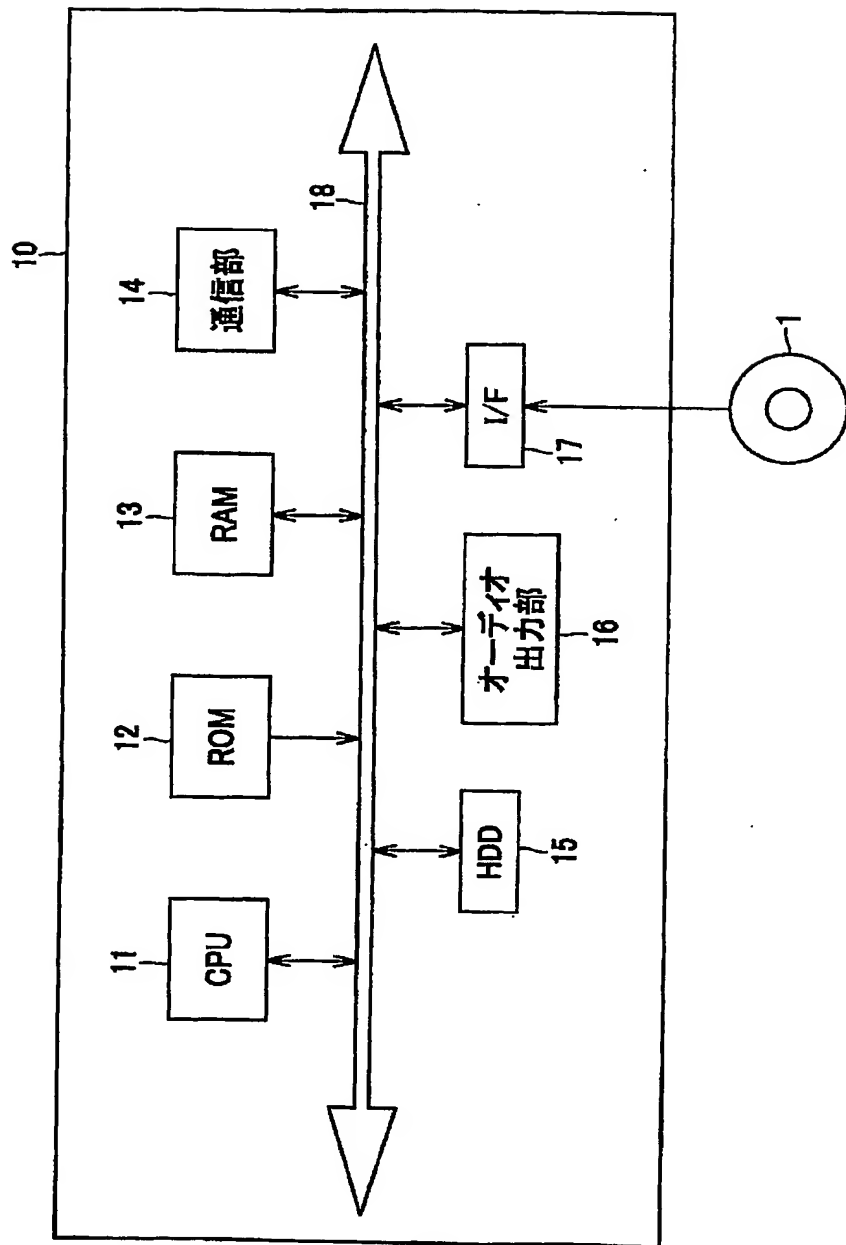
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 記録された情報の不法コピーを防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする。

【解決手段】 鍵取得モジュール 2 は、コピー防止技術が施された読み取り専用の情報記録媒体 1 に記録されている。再生モジュール 3 は、この鍵取得モジュール 2 から該鍵取得モジュール 2 に固有のメディア鍵を安全に取得し、このメディア鍵からコンテンツ鍵を生成し、このコンテンツ鍵を用いて暗号化コンテンツ 4 を復号化して再生する。ここで、鍵取得モジュール 2 は情報記録媒体 1 上に存在する必要があるが、再生モジュール 3 及び暗号化コンテンツ 4 は情報記録媒体 1 上に存在する必要はなく、情報記録媒体 1 の外部に存在していても構わない。

【選択図】 図 1



特願 2003-150906

ページ: 1/E

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更新月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社